IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. RICHARD ANTHONY DOUGHERTY, Defendant.	No. 3:23-mj-00220-KFR

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Nicholas Volpicella, being duly sworn, swear that the following is true to the best of my knowledge and belief:

1. I make this affidavit in support of a criminal complaint pursuant to Federal Rule of Criminal Procedure 3 and for Arrest Warrant pursuant to Federal Rule of Criminal Procedure 4. I submit that this Affidavit establishes probable cause to believe that RICHARD ANTHONY DOUGHERTY ("DOUGHERTY"), within the District of Alaska, beginning on an unknown date not later than January 1, 2017, and continuing until April 6, 2023, did knowingly distributed any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, in violation of Title 18, United States Code, Section 2252A(a)(2)(A); and, further, that he did knowingly possess, or knowingly accessed with

intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, in violation of Title 18, United States Code, Section 2252A(a)(5)(B).

2. I am a sworn criminal investigator with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI) and have been so employed since February 2020. I am currently assigned to the Resident Agent in Charge (RAC) office in Anchorage, AK. I am authorized as both a customs officer & immigration officer, whose duties include the enforcement of federal criminal statutes including but not limited to Titles 8, 18, 19, 21, and 31 of the United States Code. My training includes the Criminal Investigator Training Program (CITP) and the Homeland Security Investigations Special Agent Training (HSISAT) at the Federal Law Enforcement Training Center in Glynco, GA. These criminal investigative trainings included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and execution of search warrants. This training also included instruction in the law of search and seizure under the Fourth Amendment of the United States. I have also received specific training regarding investigations into the criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt,

and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. As part of these investigations, I have had the opportunity to conduct, coordinate, and/or participate in numerous investigations relating to the sexual exploitation of children. I have written and obtained search warrants related to child pornography, viewed thousands of images and videos of child pornography, and identified and conducted interviews of child exploitation suspects. Prior to my employment with RAC Anchorage as a Special Agent, I was employed as a Computer Forensic Analyst (CFA) with HSI Assistant Special Agent in Charge (ASAC) Orlando, FL, having been employed there from August 2015 – February 2020. I have performed digital forensic examinations of computer storage devices such as computers, mobile phones, hard drives, flash drives, PDAs, DVDs, CDs, and tape media. I was responsible for using all available digital evidence recovery techniques to preserve an item's authenticity and integrity while maintaining a strict chain of custody. I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images). I have also conducted and assisted with numerous local, national, and international investigations related to the possession, receipt and distribution of child pornography and other offenses involving the exploitation of children while employed as a CFA.

3. I have also been court certified / qualified as an expert witness in the field of computer forensics for the following cases:

a. *United States of America v. David R. Rivenbark* (April 2017); and.

b. *United States of America v. Terry G. Zimmerman* (November 2020).

Both cases were in the United States District Court for the Middle District of Florida. I testified as an expert witness in the field of computer forensics. My testimony covered the proper forensic processing of digital evidence and recovery of deleted evidence after years of non-use, to include the association of deleted files to specific electronic devices after the fact. Furthermore, I testified to the importance and relevancy of cashed images as it relates to knowledge and intent.

4. Based upon my training and conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography, I am aware that individuals who share and distribute child pornography are often persons who have a sexual interest in children who have escalated their activity from anonymously obtaining images of child pornography to proactively distributing images they have collected, often for the purposes of trading images of child pornography with others as a method of adding to their own collections. From my training and experience, I know that individuals involved in the distribution of child pornography also continue to obtain images of child pornography found elsewhere on the Internet, e.g. peer-to-peer networks, paid subscription sites, or free sites offering images and/or videos

5. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual

"deleted" it. I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

6. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I am familiar with the information contained in this affidavit based upon the investigation I have conducted, which included conversations communications with law enforcement officers and others and review of reports and database records, as well as my training and experience.

BACKGROUND INVESTIGATION UP TO APRIL 6, 2023

7. I submit that the information contained in this affidavit establishes probable cause to believe that Richard Anthony Dougherty (hereinafter "DOUGHERTY"), over the period of approximately 2017 until April 6, 2023, in the District of Alaska, produced, possessed, and distributed child pornography (hereinafter "CSAM"), and that such CSAM depicted three female persons under the age of 18 years at the time of production (hereinafter "MV1," "MV2," and "MV3"). Further, I submit that DOUGHERTY distributed CSAM on the internet in approximately 2017 using the username "OmniBlade."

Further, I submit that evidence establishes that a person who produces and distributes CSAM material on the internet is especially likely to highly value, preserve, and "hoard" CSAM images, and that computer technology widely available during the period of approximately 2014 until the present is likely capable of preserving files valued by the computer user for that period of time. Further, I submit that there is sufficient evidence linking DOUGHERTY to his recent use of the username "OmniBlade," his ongoing living at the RESIDENCE, his ongoing computer expertise and use, and his secrecy from his wife regarding a credit card.

CHARACTERISTIC OF PEOPLE WHO PRODUCE CSAM

8. I use the term "child pornographer" to refer to a person who produces CSAM. My knowledge of preferential sex offenders and their characteristics is based on my experience as a law enforcement officer, and other training specific to child exploitation crimes and related computer storage I have received. Based upon such training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics, which may be exhibited in varying combinations.

9. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.

10. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videos, books, slides and/or drawings or other visual media.

11. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

12. Individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer hard drive or separate digital media. Often, these secure, private locations in which child pornography are stored is on an individual's cell phone, tablet, or on a portable storage device. Each of these devices can be easily concealed. In addition, storage in some instances can be done in the "cloud," such that there are no active images or videos of child pornography located on a physical device. However, those images or videos remain accessible and in the possession of a user so long as that user has access to the internet.

13. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, e-mail addresses or telephone numbers of individuals with whom they have been

in contact and who share the same interests in child pornography. These interactions with other users can take place in person, or through mailed correspondence; however, they most often take place through various social media platforms, file-sharing services, messaging services, or through e-mail. All of these communications can be done through a computer, tablet, or cell phone.

14. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. The result is that child pornography images and images or items of child erotica can be maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. In addition, individuals may maintain collections on digital devices even after those devices have outlived their useful lives or been replaced by the user with more modern devices. I know that such devices can be stored in outbuildings, storage sheds and garages.

15. Increasingly, with faster Internet download speed and the growth of file-sharing networks and other platforms through which individuals may trade child pornography, some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic

tools. Furthermore, even in instances in which an individual engages in a cycle of downloading, viewing, and deleting images, a selection of favored images involving a particular child or act are often maintained on the device.

CHILD MOLESTERS: A BEHAVIORAL ANALYSIS

16. "Characteristics of Collection" as described in *Child Molesters: A Behavioral Analysis for Law Enforcement Officers Investigating Cases of Child Sexual Exploitation* published by the Behavioral Science Unit, Federal Bureau of Investigation, FBI Academy, Quantico, Virginia in conjunction with the National Center for Missing & Exploited Children, indicates the following[1]:

a. **Important**: The pedophile's collection is usually one of the most important things in his life.

b. **Constant:** No matter how much the pedophile has, he never has enough; and he rarely throws anything away. If police have evidence that a pedophile had a collection five or ten years ago, chances are he still has the collection now-only it is larger.

c. **Organized:** The pedophile usually maintains detailed, neat, orderly records.

d. **Permanent:** The pedophile will try to find a way to keep his collection. He might move, hide, or give his collection to another pedophile if he believes

[1] https://www.ojp.gov/pdffiles1/Digitization/149252NCJRS.pdf

the police are investigating him. Although he might, he is not likely to destroy the collection: It is his life's work.

e. **Concealed**: Because of the hidden or illegal nature of the pedophile's activity, he is concerned about the security of his collection. But this must always be weighed against his access to the collection. It does him no good if he cannot get to it.

f. **Shared:** The pedophile frequently has a need or desire to show and tell others about his collection. He is seeking validation for all his efforts.

Although this material was published in 1992, based on my training and experience, I believe this information to be accurate. Further, I believe that improvements in computer technology have increased the ease with which persons may produce, distribute, and possess CSAM.

COMPUTERS AND CHILD PORNOGRAPHY

17. Based upon my training and experience as well as my discussions with others involved in child pornography investigations, computers and computer technology have revolutionized the way in which child pornography is produced, distributed, received, and possessed. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also

required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. Now, through the use of computers and the Internet, distributors of child pornography can use various distribution networks, including but not limited to, personal email contacts, file-sharing services, list serves, and membership-based/subscription-based web sites to conduct business. These distribution networks have numerous advantages, including the ability to allow distributors to remain relatively anonymous.

18. The development of computers has also revolutionized the way in which child pornography collectors interact with each other, and sexually exploit children. Computers serve four basic functions in connection with child pornography: production, communication and distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

a. Production: Producers of child pornography can now produce high resolution still and moving images directly from a common video or digital camera. These types of cameras are ubiquitous, present on nearly every cell phone sold. Once taken, images and videos can be saved onto a computer or uploaded onto a website or attached to an email within seconds. While still on the camera or after being saved onto a computer or uploaded into a photo or video editing program, images can be edited in ways similar to how a

photograph may be altered - lightened, darkened, cropped, or otherwise manipulated. Videos can be edited or spliced together to create montages of abuse that can be several minutes to several hours long. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave a trail for law enforcement to follow. In some cases, depending upon the sophistication of the producer, it may be virtually impossible to law enforcement to determine the source of a sexually explicit image.

b. Communication and Distribution: The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. In addition, the Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the

distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer to look for "footprints" of the web sites and images accessed by the recipient.

c. Storage: The computer's capability to store images in digital form makes it an ideal repository for child pornography. Moore's law predicts that the number of transistors in a dense integrated double circuit doubles approximately every two years. In the computing world, this translates to a doubling of computer memory capacity roughly every 24 months. This increase in computer storage is reflected in the modern computer. It is not uncommon to encounter hard drives containing 1 terabyte or more of data. According to Apple, Inc., 1TB of data can hold approximately 2 million standard resolution photographs. If those images are in high-resolution format, the number decreases to 26,000. A 1TB drive can also hold 357 DVD quality movies. Storage options located outside the physical boundaries of a computer add another dimension to the equation. It is becoming increasingly common for computer users to store images in the "cloud." Services such as Google Drive, Apple iCloud, Microsoft OneDrive, and Dropbox gives users the ability to store a nearly unlimited quantity of data. The result is the ability to maintain large collections of child pornography outside of a traditional

computer, and to be able to access that collection from any device that is capable of connecting to the Internet and downloading images from the "cloud."

19. Collectors and distributors of child pornography can set up an account with a remote computing service that provides e-mail services and electronic file storage. Evidence of such online storage of child pornography may be found on the user's computer.

20. Information can be saved or stored on a computer intentionally. For example, a person may save an e-mail as a file or may save a favorite website in a "bookmark" type file. Information can also be retained unintentionally. For example, traces of an electronic communication path may be stored automatically in temporary files or Internet Service Provider client software. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Internet distributors and recipients of child pornography may be identified by examining the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient. A forensic examiner often also can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

21. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or viewed via the Internet. Even when such files have been deleted, they can often be recovered by forensic tools. When a

person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside for long periods of time in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space (free space or slack space). In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

22. As used in this warrant, the terms computer also applies to cell phones and portable tablet devices such as an iPad or Microsoft Surface. Each of the above statements regarding the use of computers to further the production, receipt and distribution of child pornography, and relating to the storage of data on a computer applies with equal force to these modern portable devices such as cell phones and tablet computers. Indeed, the computing power of these devices, as well as their portability, combined with ready access to the web through Wi-Fi networks or cellular systems has made the production, acquisition, and possession of child pornography as easy to produce, acquire, and maintain

as it has ever been, and has led to a proliferation of images available for distribution and viewing.

THE TOR NETWORK

23. The Tor network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user's web browser or by downloading the free "Tor browser bundle" available at www.torproject.org. Use of the Tor software bounces a user's communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address which could otherwise be used to identify a user. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that Tor exit node IP address. A criminal suspect's use of Tor accordingly makes it extremely difficult for law enforcement agents who are investigating a Tor Hidden Service to detect the host's, administrator's, or users' actual IP addresses or physical locations.

24. Within the Tor network itself, entire websites can be set up as "hidden services." "Hidden services" operate the same as regular public websites with one critical exception. The IP address for the web server is hidden and instead is replaced with a Tor-

based web address, which is a series of algorithm-generated characters, such as "asdlk8fs9dflku7f" followed by the suffix ".onion." A user can only reach these "hidden services" if the user is using the Tor client and operating in the Tor network. And unlike an open Internet website, is not possible to determine through public lookups the IP address of a computer hosting a Tor "hidden service." Neither law enforcement nor users can therefore determine the location of the computer that hosts the website through those public lookups.

PROBABLE CAUSE REGARDING DOUGHERTY

25. On or about October 30, 2022, the Cyber Crimes Center (C3) Child Exploitation Investigations Unit's (CEIU) Victim Identification lab, of the U.S. Department of Homeland Security, Homeland Security Investigations (HIS), received information, originally sourced from law enforcement in a foreign country, regarding two victims associated with the CSAM series known by initials that refer to the victims' actual names. The CSAM images depict what appear to be two minor pubescent females, hereafter referred to as "Minor Victim 1" ("MV1") and "Minor Victim 2" ("MV2"). The CSAM images have a create date of 2017 and depict the victims in the same bathroom at separate times, in various stages of undress, with their genitalia exposed. These images appear to have been captured by a hidden camera.

26. On March 6, 2023, a CEIU's Victim ID Lab Criminal Analyst (CA) reviewed the comments associated with the Series in Interpol's International Child Sexual Exploitation (ICSE) database. A comment posted on April 24, 2017 by a Victim

Identification Specialist (VIS) with QPS states the CSAM images were originally posted to the thread 'Star Room' on the Onion Router (Tor) board Magic Kingdom by user "OmniBlade". The user account "OmniBlade" was associated to the email address "OmniBlade@gmail.com". VIS Desirs also commented on the possibility the file names may be associated to the letters of the victims' names.

27. DOUGHERTY's Instagram account refers to what appears to be a Snapchat account with username "OmniBlade."

28. On March 6, 2023, a CA conducted a facial recognition search of MV2 which resulted in two images resembling MV2. One image depicts two adult females, one of which appears similar to MV2, wearing a necklace with what appears to be a pendant shaped with the letter of her first name. The source of the image is from a website maintained by a news publisher in Alaska of an article regarding persons in Alaska and can be found on a publicly available web page.

29. The second image resembling MV2 depicts a female standing in front of a waterfall found on a publicly available Instagram profile for a user whom I have identified as being MV2 by comparing CSAM images from this investigation with non-CSAM images available on MV2's two Instagram accounts.

30. On March 8, 2023, CA Wilson conducted further open-source research into social media profiles associated to MV2 resulting in a profile for "Richard DOUGHERTY" (Instagram username "infernumen"), matching the last name of an individual on MV2's passport applications under emergency contacts. Within DOUGHERTY's publicly

available friends list, a CA searched for any names that started with the initials associated with MV1 and located an Instagram profile containing images apparently depicting MV1. That Instagram account showed a comment indicating that MV1 and MV2 are correctly identified as sisters.

31. SA Volpicella reviewed the recovered the following number of images from the ICSE database which included images of MV1, MV2, and MV3.

a. MV1: 37 images;

b. MV2: 38 images;

c. MV3: 25 images.

I have reviewed images depicting MV1, MV2, and MV3 that I believe to contain CSAM, which is child pornography as defined by 18 U.S.C. 2256:

> (8) "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where--
>
> (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
>
> (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
>
> (C) such visual depiction has been created, adapted, or modified to appear

that an identifiable minor is engaging in sexually explicit conduct.

On April 6, 2023, I made three images that I believe to be CSAM regarding each victim (MV1, MV2, and MV3) available to the Magistrate Judge at the time of swearing the three search warrants, described below. The Magistrate Judge found that the images show sexually explicit conduct.

32. Some of the CSAM images appear to have been created by hidden camera in the vicinity of a mirror that, according to one witness, was present in the RESIDENCE as late as 2017. That is, at least some the images depict one or more victims in poses suggesting that they are unaware that the image is being created. Other CSAM images, however, appear to be "selfies" taken by the minor herself.

33. SA Volpicella also reviewed the recovered content from the Magic Kingdom board and posts requesting entry into the "Star Room". The below posts are from the user "OmniBlade":

34. 12/16/2015 at 20:14 - User OmniBlade joined Magic Kingdom

35. 01/13/2017 at 17:43 - First application into the private board "Star Room"

a. Attached one image titled "shower.jpg" sized at 559.14 KiB which is of victim MV1 or MV2.

b. OmniBlade added the message "**I have a ton of original content 10-14 to offer for access**"

36. 01/13/2017 at 20:54 – A different user wrote:

a. "For this application - NO. But if this user have a more 10-14 yo with videos

- he need to make a preview to other content, i love jailbait too and maybe YES if he have some good vids...

37. 01/13/2017 at 22:44 – A different user wrote:

    a. "Locking topic for now based on the application. If anyone wants to PM user to have him submit a better app, feel free..."

38. 01/14/2017 at 00:54 – A different user wrote:

    a. "I'll do it"

39. 01/14/2017 at 22:44 – A different user Private Messaged "OmniBlade":

    a. Subject: Application from OmniBlade

    b. [quote="OmniBlade":2359dprz]I have a ton of original content 10-14 to offer for access.

    c. Hey there, I see you applied with Star Room and I have taken the responsibility to to touch base with you and go over the application form guidelines. The application form is vague so that we can walk you through the re-application process so that you do everything right. This may take a couple attempts. So if you have the patience, I have the time. So lets get started with the Application Form Guide:

    d. Star application:

    e. All applicants post content, compressed into a rar or 7z file, password protected, no comments, no single pictures will be accepted for application, image sets and/or videos (with good quality preferably). Complete Sets, no

partials.

f. *An individuals previous contributions towards the board maybe put into consideration for acceptance into Star Room.*

g. For the application of Star room, individual images in an application form are automatically discarded and voted as NO entry. It is a good idea if you are still interested in the Star Room to re-apply with full sets (no partials) and/or a few videos. If you feel that you have what it takes to be a Star member, it is recommended that you make around 10 content posts in the main forum as this help determine your eligibility into Star Room.

h. If you have any questions please feel free to PM me or another moderator, take care, be safe, and good luck. JJB1

40. 01/23/2017 at 14:58 - Second Application with the following message:

a. "**Application to Star Forum, 2nd Attempt. This is one of the girls I have many pics/videos spanning several years. Several more girls around the same size collection. Several gigs.**"

b. "Omniblade" Shared a files via UltraShare with a password.

41. 01/23/2017 at 14:59 - Same as above, "Omniblade" seems to have double submitted the same content.

42. 01/27/2017 at 15:10 - "OmniBlade" re-applied to Star Room and added:

a. "**Hello got reply back on last app, applying with a couple more sets I have. Different girls to show variety**".

b. "OmniBlade" Shared a files via UltraShare with password of !!StarAppPasswor@#

43. Additionally, law enforcement recovered 63 other messages from "OmniBlade" across various Tor boards known to traffic CSAM to include:

a. PrincessJade, TaboolessChat, and Tenplus.

b. No files were recovered, but comments were, such as: "great posts", "thanks contributors", "amazing posts", "thanks all", etc.

c. These types of comments are indicative of the sharing of CSAM among members of a forum or board.

44. HSI Anchorage identified through open-source records that numerous social media accounts belonging to DOUGHERTY reference "OmniBlade". DOUGHERTY also has two daughters roughly the same age as MV1 & MV2 when they were photographed.

45. DOUGHERTY's current wife is a sister to the mother of MV1 and MV2. MV1 MV2's parents filed for divorce in 2017 and it's possible they lived with DOUGHERTY during that time.

46. According to the United States Air Force, Office of Special Investigations (OSI) Detachment 631, DOUGHERTY is a Technical Sergeant in the Air National Guard as part of the 176th Maintenance Group on Joint Base Elmendorf Richardson (JBER).

47. I conducted surveillance of the RESIDENCE on March 15, 2023, and observed that the RESIDENCE is a two-story residence with no visible garage doors. The color of the home is gray with white trim. The numbers "4 0 0" are displayed near the front

corner of the home closest to the front door when view from the street. A camera is visible in the front center of the home.

48. On March 20, 2023, SA Volpicella generated subpoena/summons #: HSI-AN-2023-082699 and submitted to the Google Law Enforcement Reporting Service (LERS) for review. SA Volpicella requested subscriber data / user information for the following email address: "OmniBlade@gmail.com".

49. Google LLC returned the following pertinent information (not all inclusive)

a. Google Account ID: 941239233418

b. Name: Richard Dougherty (OmniBlade)

c. Given Name: Richard

d. Family Name: Dougherty

e. e-Mail: OmniBlade@gmail.com

f. Created on: 2004-07-17 02:38:48 Z

g. Last Updated Date: 2023-03-20 11:00:31 Z

h. Last Logins: 2023-03-20 11:00:31 Z, 2023-03-19 23:36:48 Z, 2023-03-19 11:00:31 Z

i. IP Activity: 2023-03-18 06:22:34 Z (206.174.66.254) Login

j. IP address resolves back to GCI Alaska account.

I submit that the recent IP activity (i.e. March 20, 2023) and recent IP activity (i.e. March 18, 2023), indicate that DOUGHERTY continues to use computers at the RESIDENCE, where evidence indicates he has lived since 2015, and continues to use the username

"OmniBlade."

50. On April 5, 2023, SA Volpicella interviewed "Mother 1," the mother of MV1, MV2, and MV3. Mother 1 positively identified two of the three children (*i.e.* MV1 and MV2) when I showed her redacted CSAM images known to have been distributed by the user using the handle Omniblade in 2017. I did not show to Mother 1 CSAM images regarding MV3. Mother 1 also positively identified MV3 in a non-CSAM image, and I have observed that MV3 appears to be the person in both the non-CSAM image, and, also, in CSAM distributed by the user using the handle Omniblade. Mother 1 said that the bathroom depicted in the distributed CSAM images is the same bathroom as in the Premises. She recognized the color of the bathroom doors. Mother 1 also said that, during the time period of approximately 2014-2018, Mother 1, MV1, MV2, MV3, another child, and DOUGHERTY all lived at the Premises. Dougherty and LaTasha Dougherty owned the Premises.

51. Mother 1 described DOUGHERTY as an "anti-social" "recluse" who spent large amounts of time in a room used exclusively by DOUGHERTY as a "man-cave" type room. I used the phrase "man cave" in my question to Mother 1, and Mother 1 appeared to agree with that term as accurately describing a room in which DOUGHERTY possessed, accessed, and maintained a large quantity of electronic equipment, including multiple "gaming" computers and screens. Based on my training and experience, I know that the term "gaming" computer typically refers to a relatively high-value, and high-performance, computing system, capable of processing video in high-definition video desirable among

people who enjoy playing computer games. Mother 1 said that DOUGHERTY would spend time gaming or watching movies when home. When DOUGHERTY would come home from work, he would go right to "gaming" and being on the computer. Mother 1 also said that she did not know what DOUGHERTY did in the room, nor what games he played. Mother 1 said that "OmniBlade" was DOUGHERTY's email address with 100% certainty.

52. On April 6, 2023, Mother 1 said that DOUGHERTY had particular interest in MV1 and MV2 in the home, more so than his own children at the time. DOUGHERTY was very friendly, or "chummy," with the girls. Mother 1 opined that DOUGHERTY appeared to have more interest in socializing with MV1 and MV2 than with his own daughters. Mother 1 said that DOUGHERTY has two biological daughters currently living with him and those girls' mother at the Premises. Based on other information known to me, I believe those girls to currently be approximately the same age as MV1 and MV2 at the time the CSAM images were produced.

53. On April 6, 2023, SA Volpicella spoke with DOUGHERTY's commander at JBER. The commander has had direct interactions with DOUGHERTY as his commander. The commander said that DOUGHERTY is known around the squadron as the "hacker" as he has great interest in computing and gaming. DOUGHERTY is known to love computers and is very tech savvy.

PROBABLE CAUSE REGADING DOUGHERTY'S CELLULAR PHONE

54. Several of the CSAM images in this case appear to have indicia that the images were created by a user to took a "screenshot" using a smartphone. For example,

there is a speaker and a microphone icon on images. Based on my training and experience, I know that smartphones commonly have feature that allows the user to create an image preserving the contents of the screen. Further, I know that such images are commonly preserved for months or years on the phone that created the image. Also, such images are commonly transferred from the phone that was used to create the image to phones subsequently used by the same user. Based on my knowledge of the evidence in this case, I believe the screenshots were created in 2017, but, for the reasons explained herein, I submit that there is probable cause to believe that the images are likely to be found in a phone currently used by DOUGHERTY.

55. Based on my training and experience, I know that people commonly keep their cellular phones on their persons, at their homes, or in their vehicles.

EVENTS OF APRIL 6, 2023

56. On April 6, 2023, a Magistrate Judge of the United States District Court for the District of Alaska issued three warrants to search DOUGHERTY's residence in Anchorage, Alaska, his person, and his vehicle. Federal and state law enforcement executed the warrants the same date.

57. On April 6, 2023, after being advised his Miranda rights, while in the District of Alaska, DOUGHERTY confessed to producing, distributing, and possessing CSAM. DOUGHERTY described the CSAM as being "child pornography" and admitted to hoarding a collection of CSAM collected over approximately 20 years and filing terabytes of computer storage space. DOUGHERTY specifically admitted to producing CSAM by

sexually penetrating MV2 and recording the offense(s). DOUGHERTY admitted to "grooming" MV2. DOUGHERTY admitted the CSAM included images of MV1, MV2, MV3, and other minors. DOUGHERTY admitted possessing CSAM on the cellular phone seized from his person.

58. On April 6, 2023, law enforcement found evidence corroborating DOUGHERTY's confession, including, without limitation: a cellular phone hidden in the wall of one bathroom of DOUGHERTY's home, hard-wired for electricity and remotely accessed to create images of unsuspecting victims; and multiple digital devices (including a cellular phone seized from DOUGHERTY's person) containing what appears to be, upon initial review, large quantities of CSAM.

CONCLUSION

59. I submit that this affidavit supports probable cause for the attached complaint.

Respectfully submitted,

NICHOLAS G VOLPICELLA

Digitally signed by NICHOLAS G VOLPICELLA
Date: 2023.04.07 15:01:52 -08'00'

NICHOLAS VOLPICELLA
U.S. Department of Homeland Security
Homeland Security Investigations

Subscribed and sworn to before me, or remotely via phone or other reliable means, on April 7, 2023.

Kyle F. Reardon, U.S. Magistrate Judge
United States Magistrate Judge

U.S. v. DOUGHERTY
3:23-mj-00220-KFR